Section IV: Network Security
Title: Network Security and Firewalls Standard
Current Effective Date: June 30, 2008
Revision History: May 7, 2008
Original Effective Date: June 30, 2008

Purpose: To prevent unauthorized access to the North Carolina (NC) Department of Health and Human Services (DHHS) network, through the establishment of basic requirements for firewall configurations.

STANDARD

1.0 Background

Firewalls control inbound and outbound network traffic by limiting the traffic to only that which is necessary to accomplish the mission of DHHS.

2.0 Configuration and Installation

2.1 Default

By default, the statewide firewall standard is for all ports to be closed. Only those ports for which a Division and Office has written and documented business justification shall be open. Each Division and Office shall establish a process for evaluating policy and procedure changes, which at a minimum incorporates requirements for compliance to the State's Access Control Framework for communication across trust levels and emphasizes alternative methodologies to achieve full compliance. Each Division and Office will manage their own risk through this process in accordance with DHHS policies, standards, and the NC State Office of Information Technology Services (ITS) – Enterprise Security and Risk Management Office, Revision 1.7 – Risk Management Guide.

Divisions and Offices should develop firewall change request procedures to accommodate resources or events that require changes to their local firewall operations. This procedure must include a review by a firewall security analyst or subject matter expert. The procedure shall incorporate an approach to block all ports and then permit specific ports which have a business requirement while incorporating additional hardening, as necessary, to have a comprehensive security policy. *This will be accomplished by utilizing a firewall change management procedure and performed by authorized personnel only.* For temporary or emergency port openings, the Division and Office process shall establish a maximum time frame for the port to be open, not to exceed ten (10) business days. The Division and Office Information Security Official (ISO), or the entity managing the firewall, shall subsequently close the port or develop additional hardening (e.g., rule or tougher requirement). All temporary, idle sessions shall be set to time-out or close-out after one (1) hour.

2.2 Access Control

Access to firewalls shall be limited only to personnel authorized by the Division ISO or designee.

2.3 Physical Security

Firewalls shall be installed within a locked location that is physically secured from tampering or unauthorized access. Each Division ISO shall approve the physical location of the firewalls. Firewalls shall not be relocated without the prior approval of the Division ISO.

2.4 Firewall Rulesets

A firewall ruleset shall always block the following types of network traffic:

- Inbound network traffic from a non-authenticated source system with a destination address of the firewall system itself
- Inbound network traffic with a source address indicating that the packet originated on a network behind the firewall with the exception of virtual private network (VPN) traffic
- Inbound network traffic containing Internet Control Message Protocol (ICMP) traffic. PING (e.g., computer tool used to test whether a particular host is reachable across an Internet Protocol (IP) network) may be allowed but only internal to the state's network
- Inbound network traffic containing IP source routing information
- Inbound or outbound network traffic containing a source or destination address of 0.0.0.0
- Inbound or outbound network traffic containing directed broadcast addresses

3.0 Minimum Firewall Requirements

The DHHS Divisions and Offices shall enforce the following minimum firewall requirements:

- No local user accounts shall be configured on network firewalls. Only administrators responsible for the firewall may configure an account. Firewalls must use an authentication mechanism that provides accountability for the individual
- Passwords on firewalls shall be kept in a secure encrypted form
- Management of the firewall should only be conducted at the console or over an encrypted tunnel (e.g., secure socket layer (SSL) and secure shell (SSH), etc.)
- Audit logs will be enabled and reviewed following statewide standards

4.0 Monitoring and Filtering

The DHHS Divisions and Offices shall enforce the following minimum monitoring and filtering criteria:

- Logging features on Division and Office network firewalls shall capture all packets dropped or denied by the firewall. The Division and Office information technology (IT) staff, or the entity managing the firewall, shall review those error logs at least weekly to determine whether the firewall ruleset needs modification to allow applicable business function or report possible incidents. Log retention policies for firewalls shall be developed by the Divisions and Offices to satisfy internal audit requirements (i.e., federal and state compliance security regulations).
- Each Division and Office security and firewall policy shall be reviewed and verified by the Division and Office IT staff annually. If a third party entity manages the firewall, then that entity shall be responsible for reviewing and verifying the Division and Office security and firewall policy annually or when applicable.

Reference:

- NC State Office of Information Technology Services (ITS), Enterprise Security and Risk Management Office, Revision 1.7
  - Risk Management Guide

- NC Statewide Information Security Manual, Version No. 1
  - Chapter 3 – Processing Information and Document, Section 01: Networks
    - Standard 030101 – Configuring Networks
  - Chapter 3 – Processing Information and Document, Section 02: System Operation and Administration
    - Standard 030211 – Monitoring Operational Audit Logs
    - Standard 030219 – System Use Procedures

- NC State Access Control Framework

- NC DHHS Security Standards
  - Administrative Security Standards
    - Information Security Risk Management Standard
  - Network Security Standards
    - Encryption Security Standard
    - Remote Access and VPNs Security Standard

- NC DHHS Policy and Procedure Manual, Section VIII – Security and Privacy, Security Manual
  - Information Review and Auditing Policy
  - Information Technology Risk Management Policy
  - Security and Firewall Policy